IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	No. 3:24-CR-00189
v.	)	
	)	Judge Crenshaw
DAVID AARON BLOYED	)	
	)	

UNITED STATES' NOTICE OF EXPERT TESTIMONY

The United States of America, by and through undersigned counsel, hereby files this Notice of Expert Testimony pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G). The United States reserves the right to supplement these disclosures and will do so in accordance with its responsibilities to do so. In support thereof, the Government would respectfully show as follows:

I. Anthony Joseph Vesich IV, FBI Special Agent:

The Government may seek to offer expert testimony by Federal Bureau of Investigation ("FBI") Special Agent ("SA") Anthony Joseph Vesich IV. SA Vesich has been employed by the FBI as a special agent since 2019 and is currently assigned to the FBI Nashville Division as a member of the Violent Crime Unit. SA Vesich is also a certified member of the FBI's Cellular Analysis Survey Team ("CAST"), which is a specialized unit within the FBI that provides technical expertise, case consultation, and instruction in the analysis of historical call detail records, cell site location information, and other forms of geolocation information.

The Government anticipates that if called as a witness, SA Vesich will offer expert testimony, in general terms and/or as applied in this case, regarding the extraction of data from electronic devices, including the cellular telephone and laptop computer seized from the defendant in this case, as set forth more specifically below:

1. SA Vesich will testify as to his training and experience, as detailed in his

CV, including any training and experience associated with extracting data from cellular devices. SA Vesich's curriculum vitae ("CV") is attached hereto as Exhibit A and sets forth his background, training, and experience. The United States expects that it will supplement the attached CV that will identify the trials and/or depositions, if any, in which he has testified during the previous four years. SA \Vesich has not authored any relevant publications in the previous 10 years.

2. SA Vesich will testify about and explain the types of forensic extraction software available, the reliability of such software, and how such software is utilized to extract the data from electronic devices, including cellular telephones.

3. SA Vesich will testify about and explain what a cell phone extraction is; the process by which he conducts extractions from cell phones, and how the extractions are authenticated.

4. SA Vesich will testify about and describe what type of information can be extracted from a cell phone, including contacts, call logs, text messages, notes, photographs, videos, and location information. SA Vesich will further explain that such information may have metadata associated with it, including the date, time, and location associated with items of evidence recovered from these cell phone extractions as well as the type of camera used to take videos and/or photographs.

5. SA Vesich will testify that he conducted a forensic examination of the defendant's cell phone which was seized in this case. SA Vesich will testify regarding the procedures he followed to extract the data from the defendant's cell phone and will identify

the cell phone extraction. SA Vesich will identify the types of data recovered from the defendant's cell phone and explain that after he extracted the data from the cell phone, he provided an extraction of that data to other law enforcement officers involved in the investigation of this case.

6. SA Vesich will testify that he conducted a forensic examination of the defendant's computer which was seized in this case. SA Vesich will testify regarding the procedures he followed to extract the data from the defendant's computer and will identify the computer extraction. SA Vesich will identify the types of data recovered from the defendant's computer and explain that after he extracted the data from the computer, he provided an extraction of that data to other law enforcement officers involved in the investigation of this case.

The bases for SA Vesich's conclusions are (1) his years of experience as a Special Agent, and particularly his experience as a member of the Violent Crime squad; (2) his specialized training and experience as a member of the FBI's CAST; (3) and his review of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), SA Vesich has reviewed the foregoing disclosure and approves of the contents herein.

__*/s/ Anthony Joseph Vesich IV*________3/4/2025_________
Anthony Joseph Vesich IV Date
FBI Special Agent

II. **Conner Niklinski, FBI Digital Forensic Examiner:**

The Government may seek to offer expert testimony by Federal Bureau of Investigation ("FBI") Digital Forensic Examiner ("DFE") Conner Niklinski. DFE Niklinski has been employed by the FBI as a DFE since 2024 and is currently assigned to the FBI Nashville Division. Prior to his time with the FBI, DFE Niklinski served as a forensic consultant, digital forensic investigator, and digital forensic intern. DFE Niklinski's certificates and authorizations are listed on his CV, attached to this filing, but they notably include FBI Computer Analysis Response Team ("CART") Certifications for Digital Evidence Laboratory Technician and CART Technician Certification.

The Government anticipates that if called as a witness, DFE Niklinski will offer expert testimony, in general terms and/or as applied in this case, regarding the forensic imaging of data from computers, including the computer seized from the defendant in this case; what an IP address is and how investigators use IP addresses, as set forth more specifically below:

1. DFE Niklinski will testify as to his training and experience, as detailed in his CV, including any training and experience associated with extracting data from computers. DFE Niklinski's curriculum vitae ("CV") is attached hereto and sets forth his background, training, and experience, and identifies the trials and/or depositions in which he has testified during the previous four years. DFE Niklinski has not authored any relevant publications in the previous 10 years.

2. DFE Niklinski will testify about and explain the types of forensic imaging techniques and software available, the reliability of such techniques and software, and how such techniques software are used to obtain data from electronic devices, including desktop computers.

3. DFE Niklinski will testify about and explain what a forensic image is; the process by which he obtains a forensic image, reviews the forensic image, and how the

image is authenticated.

4. DFE Niklinski will testify about and describe what type of information can be imaged from a computer, including documents, images, IP addresses, browsing history, emails, log information, usernames, passwords, contacts, call logs, text messages, notes, photographs, videos, and location information. DFE Niklinski will further explain that such information may have metadata associated with it, including the date, time, and location associated with items of evidence recovered from the forensic images.

5. DFE Niklinski will testify that he conducted a forensic examination of the defendant's computer using various tools and techniques. DFE Niklinski will testify regarding the procedures he followed to image the defendant's computer and will identify the computer image. DFE Niklinski will identify the types of data recovered from the defendant's computer and explain that after he imaged the data from the computer, he provided a report of his findings to other law enforcement officers involved in the investigation of this case.

6. DFE Niklinski is expected to testify and explain what an IP address is; how IP addresses are assigned; how devices utilize IP addresses to send and receive information across the Internet; how IP addresses can be used by law enforcement to track activity by users, how law enforcement uses IP addresses to determine geographical location of users in correlation with time of day; how cyber criminals attempt to obscure their real IP address to, among other things, hide true location; how cyber criminals use VPNs to obscure their real IP address; and how IP addresses appear in logging systems commonly used in work-

from-home situations.

The bases for DFE Niklinski's conclusions are (1) his years of experience as a Digital Forensic Examiner and Consultant; (2) his specialized training and experience; (3) and his review of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), DFE Niklinski has reviewed the foregoing disclosure and approves of the contents herein.

_*/s/ Conner Niklinski*______ _3/4/2025__
Conner Niklinski Date
FBI Digital Forensic Examiner

III. Andrew McDole, FBI Computer Scientist:

The Government may seek to offer expert testimony by Federal Bureau of Investigation ("FBI") Computer Scientist ("CS") Andrew McDole. CS McDole has been employed by the FBI as a CS since August 2021 and is currently assigned to the FBI Nashville Division. CS McDole is an FBI trained computer scientist with a background in digital forensics, internet traffic analysis, computer operating systems, and data extraction. He has experience analyzing complex computer crimes.

The Government anticipates that if called as a witness, CS McDole will offer expert testimony, in general terms and/or as applied in this case, regarding the forensic imaging of data from computers, including the desktop computer seized from the defendant in this case; the purpose of VPNs; how cyber criminals use VPNs; what an IP address is and how investigators use IP addresses, as set forth more specifically below:

1. CS McDole will testify as to his training and experience, as detailed in his

CV, including any training and experience associated with extracting data from computers. CS McDole's curriculum vitae ("CV") is attached hereto as Exhibit C and sets forth his background, training, and experience, and identifies the trials and/or depositions in which he has testified during the previous four years.

2. CS McDole will testify about and explain the types of forensic imaging techniques and software available, the reliability of such techniques and software, and how such techniques software are used to obtain data from electronic devices, including desktop computers.

3. CS McDole will testify about and explain what a forensic image is; the process by which he obtains a forensic image, reviews the forensic image, and how the image is authenticated.

4. CS McDole will testify about and describe what type of information can be imaged from a computer, including documents, images, IP addresses, browsing history, emails, log information, usernames, passwords, notes, photographs, videos, and location information. CS McDole will further explain that such information may have metadata associated with it, including the date, time, and location associated with items of evidence recovered from the forensic images.

5. CS McDole is expected to testify and explain what a VPN is. Specifically, CS McDole will explain the purpose of a VPN; how a user obtains (downloads) VPN software; how a user installs VPN software; the effect that utilization of a VPN has on a user's IP address and other geolocation data; how cyber criminals use VPNs to obfuscate

their true location; and how law enforcement can discern a cyber criminal's true IP address when the actor loses or misconfigures their VPN connection.

6. CS McDole is expected to testify and explain what an IP address is; how IP addresses are assigned; how devices utilize IP addresses to send and receive information across the Internet; how IP addresses can be used by law enforcement to track activity by users, how law enforcement uses IP addresses to determine geographical location of users in correlation with time of day; how cyber criminals attempt to obscure their real IP address to, among other things, hide true location; how cyber criminals use VPNs to obscure their real IP address; and how IP addresses appear in logging systems commonly used in work-from-home situations.

The bases for CS McDole's conclusions are (1) his years of experience as a Computer Scientist; (2) his training in the field of computer science and digital forensics; and (3) his review of the facts of this case.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), CS McDole has reviewed the foregoing disclosure and approves of the contents herein.

_*/s/ Andrew McDole*__	__3/4/2025__
Andrew McDole	Date
FBI Computer Scientist	

IV. Expert Witness from SITE Intelligence Group, Intelligence Analyst:

The Government may seek to offer expert testimony provided by an expert witness employed by the SITE Intelligence Group.[1] SITE Intelligence Group ("SITE"), the world's leading non-governmental counterterrorism organization specializing in tracking and analyzing online activity of the global violent extremist community. SITE has tracked and analyzed global terrorist networks for over two decades and is well-recognized as one of the most knowledgeable and reliable experts in the field.

The Government anticipates that if called as a witness, a SITE intelligence analyst will offer expert testimony, in general terms and/or as applied in this case, regarding the domestic violent extremism groups generally, including the Goyim Defense League ("GDL"); the activities of the GDL; how the GDL recruits and operates; the extent of the GDL network; the beliefs of the GDL network; and as set forth more specifically below:

1. The SITE intelligence analyst will testify as to his training in his intelligence collection, his experience gathering open-source intelligence regarding domestic violence extremism groups, his personal knowledge regarding GDL, and his professional experience studying and collecting information regarding the GDL network.

2. The SITE intelligence analyst will testify regarding how the GDL is a national and international network of antisemitic provocateurs who espouse vitriolic antisemitism via the internet, through propaganda distributions and in street actions. He

[1] The United States is in the process of hiring this expert and will disclose the witness's identity and CV as soon as the contract paperwork to retain this expert is complete.

will also testify that GDL organizes what it calls the "Name the Nose Tour" where its members travel to cities across the country to protest in the vicinity of synagogues and walk through the downtown hubs of the cities they are in with Nazi flags and yell antisemitic slurs at any individuals they encounter.

3. The SITE intelligence analyst will testify regarding how in July 2024, members of GDL were present in the Nashville area as part of their "Name the Nose Tour 6." The SITE intelligence analyst will also testify that while in Nashville, GDL members routinely posted about their "Name the Nose Tour 6" activities on various social media platforms, including Telegram. The SITE intelligence analyst will then discuss how GDL uses various social media platforms like Telegram and Gab to communicate its activities, spread propaganda, broadcast its activities, and raise funds for its operations.

4. The SITE intelligence analysts will also provide context and background related to the GDL's publicly articulated mission statement and common themes it uses in its messaging, videos, activities, protests, and in online forums. The SITE intelligence analyst will also testify regarding various beliefs and concepts within the white nationalist community, including the book "The Turner Diaries," and associated features of that novel, including "The Day of the Rope." The SITE intelligence analyst will testify that "The Day of the Rope" is a frequently cited white-supremacist concept that originates from The Turner Diaries, a novel written by William Luther Pierce, a white nationalist, that depicts the violent overthrow of the United States government and culminates in a race war that leads to the systemic extermination of non-whites and Jews. The SITE intelligence analyst

will testify that in the novel, the "Day of the Rope" describes the day when white supremacist rebels engage in mass lynchings of purported "race traitors" such as journalists, politicians, and women in relationships with non-white men.

Consistent with the requirements of Federal Rule of Criminal Procedure 16(a)(1)(G)(v), the United States will supplement this disclosure once a specific SITE intelligence analyst has been retained, the analyst has provided their CV, and the analyst has reviewed and signed their disclosure.

V. Request for Notice of Defendants' Expert Testimony

The government hereby requests, pursuant to Fed. Crim. R. (16)(b)(1)(C) disclosure of a written summary of expert testimony the defendant intends to use as evidence at trial or at any hearing. This summary must describe the opinions of the witness, the bases and reasons therefore, and the witnesses' qualifications.

CONCLUSION

The Government asserts this notice, and the discovery provided to the defendant satisfy the requirements of Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure. If after viewing this notice and any attachment(s), the defendant requests further information or has concerns under Rule 16, the Government requests the defendant advise as to what further information is necessary to prepare for trial. The Government will supplement this notice if it discovers additional evidence that will be presented through expert opinion.

Respectfully Submitted,

ROBERT E. McGUIRE
ACTING UNITED STATES ATTORNEY

MIDDLE DISTRICT OF TENNESSEE

Date: March 4, 2025 By: *<u>/s/ Joshua A. Kurtzman</u>*
JOSHUA KURTZMAN
Assistant United States Attorney
Middle District of Tennessee